

# Mutually unbiased bases as submodules and subspaces

Joanne L. Hall\* and Jan Štoviček†

Department of Algebra

Charles University in Prague

186 75 Praha 8, Sokolovska 83, Czech Republic

\*Email: hall@karlin.mff.cuni.cz

†Email: stovicek@karlin.mff.cuni.cz

**Abstract**—Mutually unbiased bases (MUBs) have been used in several cryptographic and communications applications. There has been much speculation regarding connections between MUBs and finite geometries. Most of which has focused on a connection with projective and affine planes. We propose a connection with higher dimensional projective geometries and projective Hjelmslev geometries. We show that this proposed geometric structure is present in several constructions of MUBs.

## I. INTRODUCTION

Mutually unbiased bases (MUBs) are a structure first defined in a quantum physics context in 1960 [22]. Since then MUBs have been used in quantum key distribution protocols [3], [21], and can be used to construct signal sets for communications systems [1], [7].

A basis for  $\mathbb{C}^d$  is *orthonormal* if all basis vectors are orthogonal and of unit length. Two orthonormal bases  $\mathcal{B}_0$  and  $\mathcal{B}_1$  in  $\mathbb{C}^d$  are called *mutually unbiased* if  $|\langle\phi|\psi\rangle|^2 = 1/d$  for all  $\phi \in \mathcal{B}_0$  and  $\psi \in \mathcal{B}_1$ .

The maximum number of mutually unbiased bases in  $\mathbb{C}^d$  is  $d + 1$  [26]. A set of  $d + 1$  MUBs is called *complete*, it is complete sets of MUBs that are of most use in the communications applications. While constructions of complete sets of MUBs in  $\mathbb{C}^d$  are known when  $d$  is a prime power [26], it is unknown if such complete sets exist in non-prime power dimensions.

There has been much speculation regarding connections between MUBs and finite geometries [2], [19], [20], [25]. Most of this has focused on a connection with projective and affine planes.

The evidence for connections between MUBs and finite geometries falls into two categories: counting arguments [19], [20], and structures which construct both MUBs and finite geometries. These structures include planar functions [12], [18], symplectic spreads [11] as well as specific affine planes [8], [17].

We investigate higher dimensional projective geometries and show that some sets of MUBs may be regarded as subspaces. Note that in order for these higher order projective geometries to exist, a projective plane of the appropriate size must also exist. If all MUBs are subspaces of larger projective geometries, then a connection between MUBs and projective planes would be proven. Alas we do not go so far.

It has been shown that complete sets of MUBs are equivalent to orthogonal decompositions of the Lie algebra  $sl_n(\mathbb{C})$  [4], however finding orthogonal decompositions of Lie algebras is as difficult a task as finding sets of MUBs. Some work has been done classifying Lie Algebras using projective geometry [15], but these results have as yet not been applied to decompositions of  $sl_n(\mathbb{C})$ .

Some sets of MUBs have been show to have an Abelian group structure [10], [13]. We go further by showing that some complete sets of MUBs may be regarded as submodules of the appropriate free module, and as subspaces of a projective geometry over that module.

## II. PRELIMINARIES

### A. Constructions of MUBs

We investigate three non-equivalent constructions of MUBs. This first construction is based on planar functions over a finite field. For more on planar functions see for example [5]. Let  $\omega_p = e^{\frac{2i\pi}{p}}$ .

**Theorem 1 (Planar function construction):** [18, Thm 4.1] Let  $\mathbb{F}_q$  be a field of odd characteristic  $p$ . Let  $\Pi(x)$  be a planar function on  $\mathbb{F}_q$ . Let  $V_a = \{v_{ab} : b \in \mathbb{F}_q\}$  be the set of vectors

$$\vec{v}_{ab} = \frac{1}{\sqrt{q}} \left( \omega_p^{tr(a\Pi(x)+bx)} \right)_{x \in \mathbb{F}_q} \quad (1)$$

with  $a, b \in \mathbb{F}_q$ . The standard basis  $E$  along with the sets  $V_a$ ,  $a \in \mathbb{F}_q$ , form a complete set of  $q + 1$  MUBs in  $\mathbb{C}^q$ .

The following construction has been shown to be equivalent to the planar function construction when using  $\Pi(x) = x^2$  [9]. We highlight it as the submodule and subspaces structure appear in a different way to the planar function construction.

**Theorem 2 (Alltop Construction):** [1] [12, Thm 1] Let  $\mathbb{F}_q$  be a finite field of odd characteristic  $p \geq 5$ . Let  $V_a = \{\vec{v}_{ab} : b \in \mathbb{F}_q\}$  be the set of vectors

$$\vec{v}_{ab} = \frac{1}{\sqrt{q}} \left( \omega_p^{tr((x+a)^3+b(x+a))} \right)_{x \in \mathbb{F}_q} \quad (2)$$

with  $a, b \in \mathbb{F}_q$ . The standard basis  $E$  along with the sets  $V_a$ ,  $a \in \mathbb{F}_q$ , form a complete set of  $q + 1$  MUBs in  $\mathbb{C}^q$ .

The next construction stems from a symplectic spread.

*Theorem 3:* [11, 3.5(b)] Let  $\mathbb{F}_{p^n}$  be a field of odd characteristic  $p$ , with  $n$  odd. Let  $s$  and  $n$  be coprime, such that  $s < n/2$ . Let  $V_a = \{v_{ab} : b \in \mathbb{F}_q\}$  be the set of vectors

$$\vec{v}_{ab} = \frac{1}{\sqrt{q}} \left( \omega_p^{tr(ax+bxp^{n-s+1}+b^{p^s}x^{p^s+1})} \right)_{x \in \mathbb{F}_q} \quad (3)$$

with  $a, b \in \mathbb{F}_q$ . The standard basis  $E$  along with the sets  $V_a$ ,  $a \in \mathbb{F}_q$ , form a complete set of  $q+1$  MUBs in  $\mathbb{C}^q$ .

The next construction uses Galois rings.

*Theorem 4 (Galois ring construction):* [12, Thm 3] Let  $GR(4, n)$  be Galois ring of characteristic 4 and Teichmüller set  $\mathcal{T}_n$ . Let  $i = \omega_4 = \sqrt{-1}$ . Let  $V_a = \{\vec{v}_{ab} : b \in \mathcal{T}_r\}$  be the set of vectors

$$\vec{v}_{ab} = \frac{1}{\sqrt{2^n}} \left( i^{tr[(a+2b)x]} \right)_{x \in \mathcal{T}_n} \quad (4)$$

$a, b \in \mathcal{T}_n$ . The standard basis  $E$  along with the sets  $V_a$ ,  $a \in \mathcal{T}_n$ , form a complete set of  $2^n+1$  MUBs in  $\mathbb{C}^{2^n}$ .

These are not the only known constructions of complete sets of MUBs [11], but are good starting point for an investigation.

### B. Algebraic Structures

Let  $R$  be a ring with unity, a left  $R$ -module is an Abelian group,  $M$ , together with a product  $R \times M \mapsto M$  which satisfies the following: for all  $r_i, r_2 \in R$  and  $a_i, a_2 \in M$

$$1a = a, \quad (5)$$

$$(r_1 r_2)a = r_1(r_2 a) \quad (6)$$

$$(r_1 + r_2)a = r_1 a + r_2 a \quad (7)$$

$$r(a_1 + a_2) = ra_1 + ra_2 \quad (8)$$

This is familiar as the left axioms of a vector space. All  $\mathbb{F}$ -modules where  $\mathbb{F}$  is a field are vector spaces. Theorem 4 uses a ring to construct MUBs, hence we need the more general object of a module. We are only concerned with commutative rings, thus all modules in consideration are both left and right modules. An (left and right)  $R$  module is *free* if it is isomorphic to  $R^d$  for some  $d$ .

The trace map, familiar from finite fields, may also be used in Galois rings [24, §14]. Properties of trace map for  $GR(4, n)$  have been well studied in a coding theory context [16].

*Theorem 5:* [24, Thms 7.12, 14.34, 14.37] The trace map,  $tr : GR(p^s, n) \mapsto GR(p^s, 1)$  has the following properties:

- 1) For all  $r \in GR(p^s, 1)$  and  $x \in GR(p^s, n)$ ,  $rtr(x) = tr(rx)$ .
- 2)  $tr(\alpha) = 0$  if and only if there exists  $\beta \in R'$  such that  $\alpha = \beta - \phi(\beta)$ .

where  $\phi$  is the generalized Frobenius automorphism. Note that  $GR(p^1, n) \cong \mathbb{F}_{p^n}$ .

For further on Galois rings and fields we refer the reader to [24].

### C. Geometric Structures

The geometric structures we are investigating are projective geometries,  $PG(d-1, q)$ , defined over a finite field and projective Hjelmslev geometries  $PHG(d-1, GR(4, 1))$ , defined over a Galois ring.

Let  $M$  be an  $R$  module that is a submodule of  $R^d$ . If  $R$  is a field, then any submodule is a subspace of  $R^d$ . If  $R$  is a Galois ring then any free submodule is a subspace of  $R^d$  [14].

*Definition 6:* The projective geometry constructed from  $\mathbb{F}_q$ ,  $PG(d-1, q)$  is the set of subspaces of  $\mathbb{F}_q^d$ .  $\langle \vec{x} \rangle$  is a point of  $PG(d-1, q)$  and represents all vectors  $\rho \vec{x}$  in  $\mathbb{F}_q^d$  such that  $\rho \in \mathbb{F}_q^*$  and at least one of the entries of  $\vec{x}$  is non-zero.

*Definition 7:* [23] The projective Hjelmslev geometry constructed from  $GR(4, 1)$ ,  $PHG(d-1, GR(4, 1))$  is the set of subspaces of  $GR(4, 1)^d$ .  $\langle \vec{x} \rangle$  is a point of  $PHG(d-1, GR(4, 1))$  and represents all vectors  $\rho \vec{x}$  in  $GR(4, 1)^d$  such that  $\rho$  is a unit of  $GR(4, 1)$  and at least one of the entries of  $\vec{x}$  is a unit of  $GR(4, 1)$ .

Note that  $PG(d-1, q) \cong PHG(d-1, \mathbb{F}_q)$ .

## III. MUBS AS SUBMODULES AND SUBSPACES

### A. Conjecture

*Proposal 8:* Let  $X$  be a complete set of MUBs which contains the standard basis in  $\mathbb{C}^d$ . Let  $N$  be the set containing all the vectors from  $X$ , except the standard basis vectors. Let the vectors in  $N$  be of the form  $\alpha \omega_q^{\vec{x}}$  where  $\alpha \in \mathbb{R}$ ,  $\omega_q$  is a  $q^{th}$  root of unity, and  $\vec{x} \in \mathbb{Z}_q^d$ . Let  $\odot$  represent component wise multiplication, let

$$\vec{v} \hat{\odot} \vec{u} = \frac{\vec{v} \odot \vec{u}}{|\vec{v} \odot \vec{u}|} \quad (9)$$

and let  $N' = \{\vec{u} \hat{\odot} \vec{v}^* : \vec{u}, \vec{v} \in N\}$ ,  $M = \{\vec{x} : \alpha \omega_q^{\vec{x}} \in N\}$ , and  $M' = \{\vec{x} - \vec{y} : \vec{x}, \vec{y} \in M\}$ . Let  $U' \subset M'$  be the set containing the vectors from  $M'$  for which every entry is a non-unit, then

- 1)  $N'$  is a  $\mathbb{Z}_q$ -module.
- 2)  $M' \setminus U'$  is the set of vectors representing a subspace of a projective geometry over  $\mathbb{Z}_q$ .

We show this proposal is true for each of the constructions of MUBs mentioned in section II-A. This proposal says nothing about the existence of MUBs which are not constructed from a ring. All projective geometries and projective Hjelmslev geometries of dimension greater than 2 have an algebraic structure [6, §1.4], [14]. It may be the same for complete sets of MUBs.

MUBs for which the set of vectors forms a group under point-wise multiplication have been studied [9]. Our construction is more general in that the algebraic structure is in the set of vectors generated by point-wise multiplication.

### B. Counting

Much of the evidence for connections between MUBs and geometric structures stems from similarities in cardinality. We show that Proposal 8 is plausible in general by using cardinalities.

*Lemma 9:* Let  $q = p^n$ , with  $p$  odd, each point in  $PG(q-1, p)$  is represented by  $p-1$  vectors. The number of vectors

represented by the points in a  $(2n-1)$ -dimensional subspace of  $PG(q-1, q)$ , with the addition of  $\vec{0}$  is the same as the number of vectors in a complete set of MUBs in  $\mathbb{C}^q$  minus the standard basis.

*Proof:* Let  $X$  be an  $m$  dimensional subspace of  $PG(p^n-1, p)$  then there are  $\frac{p^{m+1}-1}{p-1}$  points, each of which may be represented by  $p-1$  different vectors. Add the vector  $\vec{0}$ .  $(p-1)\frac{p^{m+1}-1}{p-1} + 1 = p^{m+1}$ . The number of vectors in a complete set of MUBs in  $\mathbb{C}^q$ , minus the standard basis is  $p^{2n}$ . Thus if we require every vector in the set of MUBs to represent a point in the subspace, we need a  $2n-1$  dimensional subspace of  $PG(p^n-1, p)$ . ■

*Lemma 10:* Each point in  $PHG(2^n-1, GR(4, 1))$  is represented by 2 vectors. The number of vectors represented by the points in a  $2^{n-1}$  dimensional subspace of  $PHG(2^n-1, GR(4, 1))$ , with the addition of  $2^n$  vectors containing no unit elements is the same as the number of vectors in a complete set of MUBs in  $\mathbb{C}^{2^n}$  without the standard basis.

*Proof:* Let  $X$  be an  $m$  dimensional subspace of  $PHG(2^n-1, GR(4, 1))$  then there are  $2^m$  points in each of  $2^{m+1}-1$  neighbourhoods, each of which may be represented by 2 different vectors.  $2 \cdot 2^m(2^{m+1}-1) = 2^{2(m+1)} - 2^{m+1}$ , which, when we add  $2^m$  vectors which are generated by non units, is the number of vectors in a complete set of MUBs in  $\mathbb{C}^{2^{m+1}}$ , minus the standard basis. ■

### C. Odd dimensions

We now show that for specific families of MUBs proposal 8 is true.

*Theorem 11:* Let  $X$  be the complete set of MUBs in  $\mathbb{C}^{p^n}$  generated by the planar function construction (Thm 1). Let  $N \subset X$  be the set of vectors  $\vec{X} = \frac{1}{\sqrt{d}}\omega_p^{\vec{x}}$  where  $\vec{x} \in \mathbb{F}_p^r$ . Let  $M = \{\vec{x} : \omega_p^{\vec{x}} \in N\}$ , then

- 1)  $\langle N, \hat{\odot} \rangle$  is an  $\mathbb{F}_p$ -module.
- 2)  $M$  is a  $2n-1$  dimensional subspace of  $PG(p^n-1, p)$ .

*Proof:* 1. Let  $\vec{v}_{ab}$  and  $\vec{v}_{cd}$  be given as in equation (1).

$$\vec{v}_{ab} \hat{\odot} \vec{v}_{cd} = \frac{1}{\sqrt{q}} \left( \omega_p^{\text{tr}[(a+c)\Pi(x)+(b+d)x]} \right)_{x \in \mathbb{F}_q} \quad (10)$$

with  $a, b, c, d \in \mathbb{F}_q$ . Hence  $(\vec{v}_{ab} \hat{\odot} \vec{v}_{cd}) \in N$ ,  $\vec{v}_{00}$  acts as an identity element, with  $\vec{v}_{ab} \hat{\odot} \vec{v}_{((-a)(-b))} = \vec{v}_{00}$  ensuring every element has an inverse; commutativity comes from  $\mathbb{F}_q$ . Thus we have shown that  $\langle N, \hat{\odot} \rangle$  is an Abelian group (See also [10, Lem 2.84]). To show that it is a module  $\mathbb{F}_p \times N \mapsto N$ , let  $r \in \mathbb{F}_p$ . Let  $\star$  be an operation on the set  $N$  which corresponds to scalar multiplication on the set  $M$ .

$$r \star \vec{v}_{ab} = \frac{1}{\sqrt{q}} \left( \omega_p^{\text{tr}(a\Pi(x)+rbx)} \right)_{x \in \mathbb{F}_q} \quad (11)$$

with  $a, b \in \mathbb{F}_q$ . By Theorem 5

$$r \star \vec{v}_{ab} = \frac{1}{\sqrt{q}} \left( \omega_p^{\text{tr}(ra\Pi(x)+rbx)} \right)_{x \in \mathbb{F}_q} \quad (12)$$

with  $a, b \in \mathbb{F}_q$ . Hence for all  $r \in \mathbb{F}_p$  and  $\vec{v}_{ab} \in N$ ,  $r \star \vec{v}_{ab} \in N$ . The properties of  $\mathbb{F}_p$  ensure that the module axioms are satisfied.

2. Part 1. shows that  $M$  is a submodule, and thus forms a subspace of  $\mathbb{F}_p^{p^n}$ . The counting results of Lemma 10 show the size of the subspace. ■

For all  $a, b, c, d \in \mathbb{F}_q$ , any element in  $\vec{v}_{ef} \in N$  can be constructed as  $\vec{v}_{ef} = \vec{v}_{ab} \hat{\odot} \vec{v}_{cd}^*$  for some  $\vec{v}_{ab}, \vec{v}_{cd} \in N$ . Thus in the definition of Proposal 8,  $N = N'$  and  $M = M'$ . Hence Proposal 8 holds for planar function MUBs.

*Theorem 12:* Let  $X$  be the complete set of MUBs in  $\mathbb{C}^{p^n}$  generated by the Alltop construction (Thm 2). Let  $S \subset X$  be the set of vectors  $\vec{X} = \frac{1}{\sqrt{d}}\omega_p^{\vec{x}}$  where  $\vec{x} \in \mathbb{F}_p^r$ . Let  $T = \{\vec{x} : \omega_p^{\vec{x}} \in S\}$ ,  $S' = \{\vec{v} \hat{\odot} \vec{u} : \vec{v}, \vec{u} \in S\}$  and  $T' = \{\vec{x} + \vec{y} : \vec{x}, \vec{y} \in T\}$ , then

- 1)  $\langle S', \hat{\odot} \rangle$  is an  $\mathbb{F}_p$ -module.
- 2)  $T'$  is a  $2n-1$  dimensional subspace of  $PG(p^n-1, p)$ .

*Proof:* Let  $\vec{v}_{ab}, \vec{v}_{cd}$  be as defined in equation (2). We now show that  $S' = N$  and  $T' = M$ , with  $M, N$  from Theorem 11.

$$\vec{v}_{ab} \hat{\odot} \vec{v}_{cd}^* = \frac{1}{q} \left( \omega_p^{3(a-c)x^2 + (3a^2-3c^2+b-d)x + (a^3-c^3+ba-dc)} \right)_{x \in \mathbb{F}_q} \quad (13)$$

which is a quadratic in  $x$ , and hence a planar function. Theorem 11 may be used. ■

This highlights that structures which are not present in sets of vectors, may be present in another way, see also [17]. We use essentially the same proof for the MUBs generated by Theorem 3.

*Theorem 13:* Let  $X$  be the complete set of MUBs in  $\mathbb{C}^{p^n}$  generated by the construction of Theorem 3. Let  $N \subset X$  be the set of vectors  $\vec{X} = \frac{1}{\sqrt{d}}\omega_p^{\vec{x}}$  where  $\vec{x} \in \mathbb{F}_p^r$ . Let  $M = \{\vec{x} : \omega_p^{\vec{x}} \in N\}$  then

- 1)  $\langle N, \hat{\odot} \rangle$  is a  $\mathbb{F}_p$ -module.
- 2)  $M$  is a  $2n-1$  dimensional subspace of  $PG(p^n-1, p)$ .

*Proof:* 1. We use the operations  $\hat{\odot}$  and  $\star$  as in Theorem 11. From equation 3,

$$\vec{v}_{ab} \hat{\odot} \vec{v}_{cd}^* = \frac{1}{\sqrt{q}} \left( \omega_p^{\text{tr}((a-c)x + (b-d)x^{p^n-s+1} + (b^p-d^p)x^{p^s+1})} \right)_{x \in \mathbb{F}_q} \quad (14)$$

with  $a, b, c, d \in \mathbb{F}_q$ . Let  $\phi(b) = b^p$  be the Frobenius automorphism [24, §7.1], then  $b^{p^s} = \phi^{p^s-1}(b)$  and hence  $\phi^{p^s-1}(b-d) = \phi^{p^s-1}(b) - \phi^{p^s-1}(d)$ . Using this fact we can rearrange equation (14)

$$\vec{v}_{ab} \hat{\odot} \vec{v}_{cd}^* = \frac{1}{\sqrt{q}} \left( \omega_p^{\text{tr}((a-c)x + (b-d)x^{p^n-s+1} + (b-d)^{p^s}x^{p^s+1})} \right)_{x \in \mathbb{F}_q} \quad (15)$$

with  $a, b \in \mathbb{F}_q$ . Showing that  $\vec{v}_{ab} \hat{\odot} \vec{v}_{cd}^* \in N$ . As with Theorem 11, we use the operation  $\star$  and see that  $N$  is an  $\mathbb{F}_p$  module.

2. The proof is the same as for Theorem 11. ■ As with Theorem 11, we find that  $M = M'$  and  $N' = N$  for  $M, M', N, N'$  as in Proposal 8.

These three structures based on finite fields all conform to the structure of Proposal 8.

## D. Even dimensions

*Theorem 14:* Let  $X$  be the complete set of MUBs in dimension  $d = 2^n$  generated by the Galois ring construction [12]. Let  $N \subset X$  be the set of vectors  $\vec{X} = \frac{1}{\sqrt{d}} i^{\vec{x}}$  where  $\vec{x} \in GR(4, 1)^{2^n}$ . Let  $M = \{\vec{x} : i^{\vec{x}} \in N\}$ , then

- 1)  $N$  is a  $GR(4, 1)$ -module.
- 2)  $M$  is a  $2^{n-1}$  dimensional subspace of  $PHG(2^n - 1, GR(4, 1))$ .

*Proof:* 1. Let  $\alpha = a + 2b$ , and  $\beta = c + 2d$  where  $a, b, c, d \in \mathcal{T}_n$  the Teichmüller set of  $GR(4, n)$ . Then equation (4) becomes

$$\vec{v}_\alpha = \frac{1}{\sqrt{2^n}} \left( i^{tr[\alpha x]} \right)_{x \in \mathcal{T}_n} \quad (16)$$

$\alpha \in GR(4, n)$ . Let  $\hat{\alpha}$  be as in Proposal 8

$$\vec{v}_\alpha \hat{\alpha} \vec{v}_\beta = \frac{1}{\sqrt{2^n}} \left( i^{tr[\alpha + \beta x]} \right)_{x \in \mathcal{T}_n} \quad (17)$$

$\vec{v}_\alpha \hat{\alpha} \vec{v}_\beta \in M$ .  $\vec{v}_0$  is the identity,  $\vec{v}_\alpha \hat{\alpha} \vec{v}_{-\alpha} = \vec{v}_0$  showing inverses, and commutativity is given by the properties of Galois rings.

Let  $\star$  be the operation  $GR(4, 1) \times N$  that corresponds to scalar multiplication on  $M$ .

$$\begin{aligned} r \star \vec{v}_\alpha &= \frac{1}{\sqrt{2^n}} \left( i^{r tr[\alpha x]} \right)_{x \in \mathcal{T}_n} \\ &= \frac{1}{\sqrt{2^n}} \left( i^{tr[r\alpha x]} \right)_{x \in \mathcal{T}_n} \end{aligned} \quad (18)$$

and hence  $r \star \vec{v}_\alpha \in M$ , for all  $r \in GR(4, 1)$ . Hence  $M$  is a submodule.

2. Part 1. shows that  $M$  is a module. To show  $M$  is free we need that for every  $\vec{v}$  such that  $2\vec{v} = 0$ , there exists  $\vec{u}$  such that  $2\vec{u} = \vec{v}$ . Thus we require that if  $\alpha$  is such that

$$2tr(\alpha x) = tr(2\alpha x) = 0 \quad (19)$$

for all  $x \in \mathcal{T}_n$ , then there exists  $\beta \in M$  such that  $\alpha = 2\beta$ . Reverting to the p-adic notation, let  $\alpha = a + 2b$  and  $\beta = c + 2d$ , then  $2\alpha = 0 + 2a$  and  $2\beta = 0 + 2c$ . Hence we need to show that if  $tr(2\alpha x) = 0$  for all  $x \in \mathcal{T}_n$ , then  $a = 0$ .

Using Theorem 5.2, we see that this is equivalent to showing that for all  $x \in \mathcal{T}_n$ , there exists  $\gamma = (e + 2f) \in GR(4, n)$  such that

$$2ax = e + 2f - \phi(e + 2f) \quad (20)$$

$$2ax = e + 2f - e^2 - 2f^2 \quad (21)$$

where  $a, x, e, f \in \mathcal{T}_n$ . This simplifies to

$$ax = f - f^2 \quad (22)$$

If  $a = 0$ , then we have solved our problem. Assume  $a \neq 0$ , then there exists  $x \in \mathcal{T}_n$  such that  $ax = 1$ . Thus we require a solution to

$$0 = f^2 - f + 1 \quad (23)$$

This is a monic irreducible polynomial of degree 2, and hence has possible solution only in  $GR(4, 2)$ . Let  $h(f) = f^2 - f + 1$ ,

then  $GR(4, 2) = \mathbb{Z}_4[f]/(h(f))$ , and hence  $\mathcal{T}_2 = \{0, 1, \xi, \xi + 3\}$  where  $\xi$  is a root of  $h(f)$ . From equation (22)

$$\xi - \xi^2 = \xi - \xi - 3 = 1, \quad (24)$$

$$\xi^2 - \xi^4 = \xi^2 - \xi = 3. \quad (25)$$

Hence if  $ax \in \{\xi, \xi + 3\}$  then equation (22) has no solution. We require that equation (22) holds for fixed  $a$  and all  $x \in \mathcal{T}_n$ , hence we require that  $a = 0$ , which shows that  $M$  is a free submodule. And thus by construction forms a subspace of  $PHG(2^n - 1, GR(4, 1))$ . The counting results of Lemma 10 show the size of the subspace. ■

Note that  $GR(p^s, 1) \cong \mathbb{Z}_{p^s}$ , and as with Theorem 11,  $M = M'$  and  $N = N'$ , thus the conditions of Proposal 8 are satisfied.

## IV. CONCLUSION

We have shown that several sets of MUBs display the algebraic structure of a module and the geometric structure of a subspace of a projective Hjelmslev geometry. There are also counting results to show that this geometric structure may be true in general. Of particular note is that these structures may not arise from the sets of vectors which define the MUBs, but from the sets of vectors derived from component wise multiplication.

We have not covered all possible constructions of MUBs, but have shown sufficient evidence that this is a structure worthy of more thorough investigation.

## REFERENCES

- [1] W.O. Alltop. Complex Sequences with low periodic correlations. *IEEE Transactions on Information Theory*, 26(3):350–354, 1980.
- [2] Ingemar Bengtsson. Mubs, polytopes, and finite geometries. *AIP conference Proceedings*, 750:63–69, 2005.
- [3] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 1984.
- [4] P.O. Boykin, M. Sitharam, P.H. Tiep and P. Wocjan Mutually Unbiased Bases and Orthogonal Decompositions of Lie algebras. *Quantum Information and Computation*, 7(4): 371–382, 2007.
- [5] R.S. Coulter and R.W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Designs, Codes and Cryptography*, 10(2):167–184, 1997.
- [6] P. Dembowski. *Finite Geometries*. Classics in Mathematics. Springer, reprint of the 1968 edition, 1997.
- [7] C. Ding and J. Yuan. Signal Sets From Functions With Optimum Nonlinearity. *IEEE Transactions on Information Theory*, 55(5):936–940, 2007.
- [8] K.S. Gibbons, M.J. Hoffman, and W.K. Wootters. Discrete phase space based on finite fields. *Physical Review A*, 70(062101):1–23, 2004.
- [9] C. Godsil and A. Roy. Equiangular lines, mutually unbiased bases, and spin models. *European Journal of Combinatorics*, 30(1):246–262, 2009.
- [10] Joanne L. Hall. *Mutually unbiased bases and related structures*. PhD thesis, RMIT University, 2011.
- [11] W. M. Kantor. Mubs, inequivalence and affine planes. *Arxiv*, 1104.3370v2, July 2011.
- [12] A. Klappenecker and M. Rötteler. Constructions of Mutually Unbiased Bases. *Lecture Notes in Computer Science*, 2948:137–144, 2003.
- [13] A.B. Klimov, C. Muñoz, and J.L. Romero. Geometrical approach to the discrete Wigner function in prime power dimensions. *Journal of Physics A: Mathematical and General*, 39(46):14471–14497, 2006.
- [14] A. Kreuzer. A system of axioms for projective Hjelmslev spaces. *Journal of Geometry*, 40(1-2):125–147, 1991.
- [15] J.M. Landsberg and L. Manivel. Construction and classification of complex simple Lie algebras via projective geometry. *Selecta Mathematica, New Series*, 8:137–159, 2002.

- [16] Alexander A. Nechaev and Alexey S. Kuzmin. Trace-function on a Galois ring in coding theory. *Lecture Notes in Computer Science*, 1255:227–290, 1997.
- [17] A. Rao, D. Donovan, and J.L. Hall. Mutually orthogonal Latin squares and mutually unbiased bases in dimensions of odd prime power. *Cryptography and Communications*, 2(2):221–231, 2010.
- [18] A. Roy and A.J. Scott. Weighted complex projective 2-designs from bases: Optimal state determination by orthogonal measurements. *Journal of Mathematical Physics*, 48(072110):1–24, 2007.
- [19] M. Saniga and M. Planat. Hjelmslev geometry of mutually unbiased bases. *Journal of Physics A: Mathematical and General*, 39(2):435–440, 2006.
- [20] M. Saniga, M. Planat, and H. Rosu. Mutually unbiased bases and finite projective planes. *Journal of Optics B: Quantum and Semiclassical Optics*, 6:L19–L20, 2004.
- [21] V. Scarani, A. Aćin, G. Ribordy, and N. Gisin. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Physical Review Letters* 92 (5) 057901, 2004.
- [22] J. Schwinger. Unitary Operator Bases. *Proceedings of the National Academy of Sciences of the United States of America*, 46(4):570–579, 1960.
- [23] F.D. Veldkamp. Handbook of incidence geometry. chapter Geometry over Rings, pages 1033– 1084. Elsevier Science, 1995.
- [24] Z.X. Wan. *Finite Fields and Galois rings*. World Scientific, Singapore, 2012.
- [25] W. Wootters. Quantum Measurements and Finite Geometry. *Foundations of Physics*, 36(1):112–126, 2006.
- [26] W. Wootters and B. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363–381, 1989.